selected based on the particular user profile associated with client system 10 as defined in client authorization database 100, or can instead be selected to cause the reauthorization procedure to be repeated after a standard period of time.

A service message generator 118 then mathematically combines random number 108, authorization code 112, and new expiration count 116 to generate a service message. Since authorized server system 60 has successfully decrypted the client message, the service message generated thereby includes the same random number as the client message. The service message is encrypted by service message encryptor 120 using an encryption key 122. The resulting encrypted service message is transmitted to client system 10 via network interface 55.

Reference is now made to Figure 4, which illustrates elements of message comparison subsystem 76 according to this embodiment of the invention. The service message is received by a service message decryptor 124, which decrypts the message using a decryption key 126. A service message decombiner separates the service message into its constituent parts, which include the authorization code, the new expiration count, and the random number. The random number included in the service message is passed to random number comparator 130, where it compared with the random number included in the client message. If it is determined that the random numbers are the same, client system 10 assumes that server system 60 has decrypted the message and is therefore authorized to provide network resources to the client. If, however, client system 10 receives no service message or does not receive the original random number in the service message, the client system assumes that the server system is unauthorized.

If the server system is found to be authorized, client system enables or activates its functions based on the value of the authorization code. An appropriate authorization code

WORKMAN, NYDEGGER & SEELEY
A PROFESSIONAL CORPORATION
ATTORNEYS AT LAW
1000 EAGLE GATE TOWER
60 EAST SOUTH TEMPLE
SALT LAKE CITY, UTAH 84111

written to a control register in an application-specific integrated circuit, such as ASIC 30 of Fig. 2, permits the functions of the client system to operate. The authorization code can further indicate one of any number of levels of service or functionality. For example, when the invention is practiced in a WebTV set-top box or another client system that provides information and entertainment services to a user, the authorization code may activate the particular services that the user has subscribed to. Likewise, the new expiration count is written to a control register at the client system so as to again initiate the server verification procedure described herein when the security count exceeds the new expiration count.

If the server system has been determined to be unauthorized, grace period timer 90 of Figure 4 will eventually indicate that the allotted grace period has expired. At this point, the non-essential or any other set of functions of client system 10 are disabled until such time that an authorized server system is identified.

Figure 6 illustrates an embodiment of the invention wherein the authorization code and the new expiration count are written to control registers at an ASIC in a secure manner that essentially eliminates the opportunity of operators of the client system to override or otherwise tamper with the security features described herein. As has been described in reference to Figure 2, ASIC 30 is connected to a display device 20 and one or more memory devices 132. ASIC 30 can receive service messages and other information from the server system by means of network infrastructure 52 and network interface 54.

One of the functions of CPU 28 is writing control parameters to control registers 134 of ASIC 30. Among the control parameters are the authorization code and the new expiration count. According to this embodiment, CPU 28 transmits the authorization code and the new expiration count to ASIC 30 in the encrypted form in which they were received from the server system. A private decryption key 126 is encoded on ASIC 30 and permits a

WORKMAN, NYDEGGER & SEELEY
A PROFESSIONAL CORPORATION
ATTORNEYS AT LAW
1000 EAGLE GATE TOWER
60 EAST SOUTH TEMPLE
SALT LAKE CITY, UTAH 84111

decryptor 124 encoded on ASIC to perform decryption of the authorization code and the new expiration count. It is noted that decryption key 126 and decryptor 124 of Figure 6 can be the same as the corresponding elements illustrated in Figure 5. Once the client system determines that the server system authorized, the new expiration count and the authorization code, having been decrypted, are written to secure registers 134b. In this manner, authorized server system 60 can securely write the new expiration count, the authorization code, and any other security parameters to secure control registers 134b without software operating on the client system having access to decryption key 126. Control parameters that do not pertain to the security features of the invention can be written to non-secure control registers 132a included in ASIC 30.

As illustrated in Figure 6, the security system of the invention can allow operating system software or other software operating on the client system to see only a limited amount of information. For example, as discussed herein, the authorization code and the expiration count can be written to secure control registers 134b. In addition, the authorization interrupt signal generated by count comparator 88 of Fig. 4 can be written to a control register 132 in one embodiment. Otherwise, the operation of the security system of this embodiment of the invention is not visible to the operating system, but is instead conducted by transmitting encrypted messages between the client system and the server system and decrypting the service message using a decryption key 126 encoded in hardware at the client system. Accordingly, rogue software or operators of the client system are unable to interfere with the operation of the security features of the invention.

Figure 7 illustrates an alternative embodiment, wherein the communication between the client and server is facilitated by an intelligent peripheral. As used herein, "intelligent peripheral" refers to any object or device associated with the client system, whether

WORKMAN, NYDEGGER & SEELEY
A PROFESSIONAL CORPORATION
ATTORNEYS AT LAW
1000 EAGLE GATE TOWER
60 EAST SOUTH TEMPLE
SALT LAKE CITY, UTAH 84111